Journal of Network and Innovative Computing
ISSN 2160-2174 Volume 4 (2016) pp. 095-105


# Information System Security Risk Management improvement

**Wissam ABBASS[1], Amine BAINA[2] and Mostafa BELLAFKIH[3]**

RAI2S Team, STRS Laboratory
National Institute of Posts and Telecommunications - INPT
Rabat, Morocco
*{abbass, baina, mbella}@inpt.ac.ma*

***Abstract*: Nowadays, the business services of organizations depend widely on Information Systems (IS). However, these systems may face potential failure or risks that could lead to a business failure. Therefore, the Information System Security Risk management (ISSRM) in organizations is ultimate for business success. ISSRM protects the information availability, integrity, and privacy. The aim of this paper is to improve the ISSRM domain model through the security oriented modeling languages and the enterprise architecture. For this purpose, a survey of the ISSRM alignment in comparison with the security modeling languages is first outlined followed by an overview of the enterprise architecture benefits that can positively influence the ISSRM process.**

***Keywords*:** Information System Security Risk Management; Information System Security Risk alignment; Security modeling; SecureUML; Mal-Activity Diagrams; Misuse Cases; Secure Tropos; Entreprise architecure risk management.

## I. Introduction

The Critical Information Infrastructures (CIIs) are the basis of our daily life, connecting cities and countries to form a modern society [1]. Their disruption or destruction would have cascading impacts on national security, public safety and the global economy. CIIs represent the core base on which other critical infrastructures depend, hence the need to identify all the potential risks that may influence their proper functioning. A CII comprises of assets (whether physical or virtual) that provide vital services [2]. Usually, an asset represents an information system and/or facilities such as computer hosts, services or corporate offices modeled as collections of LANs which are linked by a WAN.

Organizations create value by processing information. The quality of that information is vital in making operational decisions. This same information is managed by information systems hence the importance of their reliability. Therefore, attacks against information systems may dramatically impact the integrity of sensitive information and the availability of provided services. In order to reach a reliable information system, organizations should conduct a Risk Management (RM) [3]. RM can eliminate or at least reduce the potential risks and determine the necessary countermeasures to ensure the security of sensitive information.

Organizations sustainable development depends widely on Information Systems (IS) hence the value of their security [4]. In fact, security aspects allow efficient usage of IS and enhanced business performance. Information Systems Security helps resisting potential risks. Security requirements are usually considered only after the definition of the business services. Actually, the IS Security Risk Management (ISSRM) methods (MEHARI [5], EBIOS [6], CRAMM [7], OCTAVE [8]…) do perform security needs until the final stages (implementation and/or maintenance). These ISSRM methods are considered as rigorous methodological tools that help taking rational decisions for IS Security. Additionally, their results are generally informal and not sufficiently analytical; it consists of documents in natural language (texts and tables). This lack of formality prevents the reasoning, evolution and traceability of ISSRM related information [9]. To prevent the problem of using informal documents, it is best to take advantage of the benefits of models. This gap between security requirements and business security needs can be improved by aligning RM concepts with those of conceptual modeling languages [10]. Furthermore, ISSRM methods are applied once the architectural design is defined which is the opposite of the IS development. Thus, ISSRM is not aligned with the security requirements.

Our view is that a modeling approach would improve ISSRM. Models allow achieving a better formality and quality in the representation of the information. The modeling concept is a growing concern among various organizations. It is an activity of representing an organization processes in order to be analyzed and improved. Models could help organizations reach a tolerable level of security by identifying security holes and mishandlings [11]. They can also support the reasoning, evolution and traceability of ISSRM related information. In

addition, the modeling approach could allow linking business assets with security risk management and representing ISSRM using different perspectives. Modeling will raise the ability to identify and manage risks faced by organizations no matter their size. For this reason, organizations must understand the variables that may affect their operations, thus classifying, managing, and mitigating risk factors.

Enterprise Architecture (EA) encompasses capabilities: processes, technologies, and information that may likely be threaten by diverse factors. EA promotes methodical analysis and understanding of complex cases that may an organization security face.

The paper is organized as follow: Section II establishes a survey of the literature. Section III introduces the ISSRM and the security modeling languages alignment. Section IV discusses benefits, completeness and limitations of the obtained alignments. Finally section V presents the conclusion and the future work.

## II. Survey of the literature

The survey of the literature is divided into three parts. The first and the second part detail the ISSRM domain model and its process. The third part assesses the security modeling languages. Those are candidate for comparison with the ISSRM domain model.

### *A. ISSRM domain Model:*

ISSRM domain model addresses the security strengths related to IS domain [12]. The domain model is a result of a thorough survey of the Risk Management standards, security related standards and Security Risk Management methods. ISSRM is not specific to one organization but covers the Security Risk Management of all organizations considering their assets, risks and their treatment.

The ISSRM domain model is shown in Figure 1. It consists of three fundamental concepts:

- **Asset-related concepts:** it describes the critical assets and their security criteria. An asset (whether physical or virtual) provides vital services for the organization. Business assets include information, processes, and capabilities of value for the business. IT assets are components of the information system that supports business assets. A security criterion represents a constraint (security needs) on business assets describing generally the need for confidentiality, integrity and availability.
- **Risk-related concepts:** it depicts the components of risk (threat, vulnerability, impact). An event is the combination of a threat and one or more vulnerabilities. A threat agent is an agent that may cause harm to IS assets. An attack method is the manner by which a threat agent accomplishes a threat. The risks target business objectives and attack IS assets to paralyze the fulfillment of business services.
- **Risk treatment related concepts:** it defines the risk treatment decisions. Risk treatments: shows the risk handling in order to improve the security requirements. Security requirements express the countermeasure. Control: Counter attack (Security practices) that would lessen the risk impact.

### *B. ISSRM process:*

The ISSRM process helps manage risks by choosing the adequate controls to avoid threats, eliminate vulnerabilities and reduce the potential impact. It consists of the following steps:

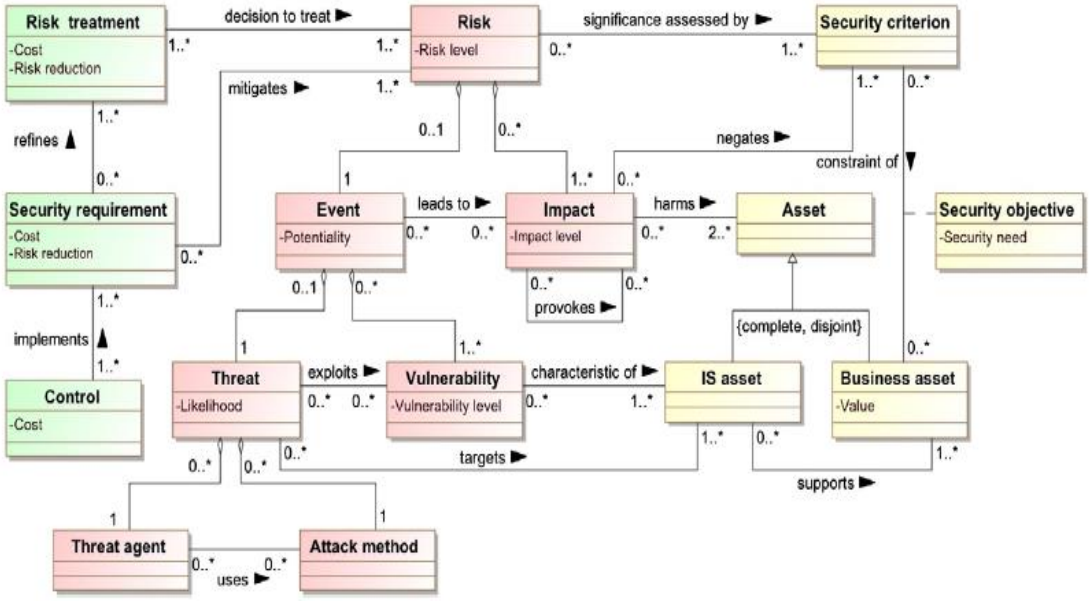


**Figure 1.** The ISSRM domain model [13]

1. Asset identification: identification of the IS assets and Business assets;

2. Security objectives determination: establishing the security criteria;
3. Risk assessment: determining the risk components : threat, threat agent, attack method, vulnerability and impact;
4. Risk treatment decisions;
5. Security requirements definition;
6. Control selection;
7. Control implementation.

Figure 2 introduces the steps of the ISSRM process in general.

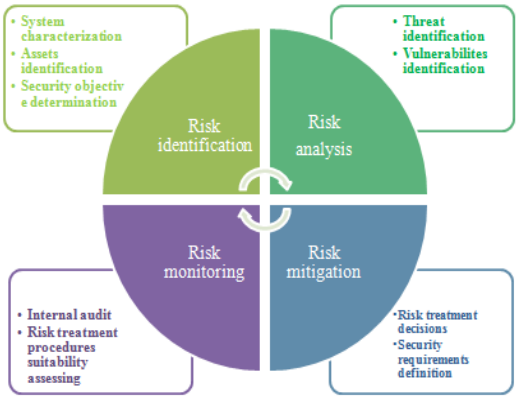


**Figure 2.** The ISSRM process

### C. *The security modeling languages:*

The security modeling languages allow the identification and the treatment of potential risks that may occur during different stages of development, implementation or maintenance phases.

- **SecureUML** [14] [15]: It is a modeling language that annotates UML models with information relevant to access control. It can be used in the context of a model-driven software development process to generate access control infrastructures.
- **Secure Tropos** [16] [17]: Secure Tropos is an extension of Tropos [18]. It is based on the concept of security constraint. It also includes security entities that represent the concepts of dependency, goal, task, resource, and capability. These entities are used to describe a security attack scenarios. Secure Tropos combines requirements engineering concepts with security engineering concepts under a unified process to support the analysis and development of secure systems.
- **Mal-Activity Diagrams** [19] [20]: Malicious-Activity Diagrams extend the concepts of Activity diagrams. It allows the inclusion of the security aspects (malicious actor, malicious activities; malicious decisions) in the UML Activity Diagrams.
- **Misuse Cases Diagrams** [21] [22]: Mis-Use Cases Diagram extends the concepts of the UML Use Cases Diagrams. It improves the Use cases with security oriented extension. It consists of misuse case, a misuser (attacker) and the relationships: Threaten or/and Mitigates.

### D. *Enterprise risk management:*

Security models guide organizations to determine the actions that will embrace the opportunity of managing risk. EA is the combine between business and IT; it's the means for aligning business and IT within an organization.

Enterprise Risk Management (ERM) [23] proposes that organizations address all their risks comprehensively and coherently, instead of managing them individually. ERM represents a significant evolution for risk management such as:

- Includes organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc…);
- Manages the organizational exposures to risk as an interconnected risk portfolio rather than as individual "silos";
- Assesses the interconnected risk portfolio in the context of all significant internal and external circumstances;
- Grants a structured process for the management of all risks, either quantitative or qualitative;
- Embeds risk management as a significant component in all critical decisions of the organization.

ERM is the discipline by which organizations monitor, analyze, and control risks from across its architecture, with the aim of optimizing the risk-taking behavior in a portfolio context. Unlike traditional RM where individual risk categories are separately managed in risk "silos," ERM enables organizations to manage a wide array of risks in an integrated, enterprise-wide fashion. ERM is a holistic approach to organizations architecture with the aim of modeling the role of IT systems in the organization, aligning IT services with business processes. Nevertheless, ERM can be considered as a compliance exercise that provides solid guidance for executive decision-making.

## III. ISSRM and security modeling languages Alignment

This section highlights the significance of the alignment of ISSRM and security modeling languages. The significance of this alignment is to improve these languages in order to support the ISSRM process [24].

Several alignments for enhancing ISSRM are proposed in the literature. This paper aims at understanding these alignments, their strengths and weaknesses. For this purpose, we review four alignments including the security modeling languages previously mentioned in the section II (SecureUML, Secure Tropos, Misuse Case Diagrams and Mal-activity Diagrams) and compare them. The comparison is based on concepts, modeling, and processes criteria.

### A. *ISSRM and Secure Tropos Alignment:*

Matulevicius and Mayer [25] have investigated the alignment between Secure Tropos and the ISSRM domain model.

In the chosen example, the concepts of security entities: security constraint, secure dependency, and security goal, task and resource are used. Secure Tropos allow modeling crutial assets and their security criteria [26].

Table 1 summarizes the advantages and disadvantages of Secure Tropos.

| Advantages | Disadvantages |
|---|---|
| - Identification of the crucial assets.<br>- Availability of security concepts (constraint, security goal). | -The constructs are used to model more than one of the ISSRM concepts.<br>-No constructs semantics is provided.<br>-No usage guidance. |

*Table 1.*The advantages and disadvantages of Secure Tropos

Secure Tropos supports risk in general unlike ISSRM model which focuses on the IS security.

All the steps of the ISSRM process are conducted by Secure Tropos expect control implementation.

### *B. ISSRM and Mal-Activity Diagrams Alignment:*

The alignment provided by [27] introduce many holes between Mal-Activity Diagrams and the ISSRM domain model. Actually, like Secure Tropos Mal-Activity Diagrams do not provide its constructs semantic. Furthermore, almost all the ISSRM concepts are not covered by the Mal-Activity Diagrams constructs.

Table 2 reviews the advantages and disadvantages of Mal-Activity Diagrams.

| Advantages | Disadvantages |
|---|---|
| - Take into account risk treatment decisions.<br>- Detailed description of the threat scenario ( attack method). | -No security aspects included.<br>-Security criterion construct is not covered.<br>-No usage guidance. |

*Table 2.*The advantages and disadvantages of Mal-activity diagrams

Assets identification, risk assessment, risk treatment and security requirements definitions of the ISSRM process are employed by Mal-Activity Diagrams.

### *C. ISSRM and Misuse Cases Diagrams Alignment:*

The contribution in [28] helps modeling and analyzing the system from an attacker (misuser) perspective which increases the chance of identifying threats that would have been ignored. Malicious behaviors are modeled by misuse cases that target use cases and countermeasures as security use cases that mitigate misuse cases. It can better model threat agent and attack method than the Secure Tropos, SecureUML and Mal-Activity Diagrams.

However, this alignment does not consider how a misuse targets a usecase, why a misuser attacks a usecase, and impacts of a security usecase on another. IS assets and Business assets both are represented using the use case and actor concepts. An additional confusion it does not consider vulnerabilities and it is essential for identifying all possible threats and attacks.

Table 3 involves the advantages and disadvantages of Misuse Cases Diagrams.

| Advantages | Disadvantages |
|---|---|
| - Perform a modeling based on the attacker point of view.<br>- Detailed description of the threat agent and method. | -Do not include a modeling constrcuts to model the attacker intention and the threat impacts.<br>-Modeling IS and Business assets is confusing.<br>-No usage guidance. |

*Table 3.*The advantages and disadvantages of Misuse cases diagrams

Misuse Cases Diagrams dress assets identification, risk assessment, security requirements definition.

### *D. ISSRM and SecureUML Alignment:*

The alignment in [29] reflects a modeling based on authorization constraints. It contributes to the annotating of UML models with access control vocabulary. The alignment only describes information relevant to access control.

Table 4 involves the advantages and disadvantages of SecureUML.

| Advantages | Disadvantages |
|---|---|
| - Focuses on access control relation information.<br>-Provides authorization constraints and the concept of roles.<br>- Perform a modeling based on the administrator ( protector) perspective. | -Does not support Vulnerability and impact.<br>- No control implementation is conducted.<br>-Controls Selection are partially supported.<br>-No usage guidance. |

*Table 4.*The advantages and disadvantages of SecureUML

Regarding the ISSRM process, SecureUML covers the asset identification, risk assessment and Security requirements definition.

Table 5 details the ISSRM alignment and the chosen security modeling languages.

Table 6 shows the steps of the ISSRM process covered by the security modeling languages.

| *ISSRM domain model concepts* | *Secure Tropos Constructs* | *Mal-Activity Diagrams Constructs* | *Misuse cases Diagrams Constructs* | *SecureUML Constructs* |
|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Assets-related concepts** | Asset | | - | | ModelElement class |
| | Business Asset | Actor, goal, softgoal, plan resource | Activity, controlflow, decision | Actor and use case | Attributes of a class ModelElement |
| | IS Asset | | Activity, controlflow, decision, swimlane | | Role class, an association permission, an operation of the class ModelElement |
| | Security criterion | Softgoal, security constraint | - | - | - |
| | Risk | - | - | - | - |
| **Risk-related concepts** | Threat | Goal, plan | Mal-swimlane | Misuser and misuse case | Role class, an association permission |
| | Threat agent | Actor | Mal-swimlane, mal activities, mal-decision, mal-swimlane | Misuser | Role class |
| | Attack method | Plan, attacks relationship | Mal activities, mal-decision, Mal-swimlane | Misuse case | Attributes of the association permission |
| | Vulnerability | Belief | - | - | - |
| | Impact | Contribution between threat and softgoal | Mal activities | - | - |
| | Event | Threat | - | - | - |
| | Risk treatment | - | - | - | - |
| **Risk treatment related concepts** | Security requirement | Actor, goal, softgoal, plan resource, security constraint | MitigarionActivity, MitigationLink | Use case | Authorization, constraint, contrainedElement |
| | Control | New model | Swimlane | - | New model ( the whole model is considered as control) |

*Table 4.*The ISSRM and security modeling languages modeling alignment

| ***Security Languages*** / ***ISSRM process*** | ***SecureUML*** | ***Mal-Activity Diagrams*** | ***Misuse Cases Diagrams*** | ***Secure Tropos*** |
|---|---|---|---|---|
| **Asset identification** | X | X | X | X |
| **Security objectives determination** | | | | X |

| | | | | |
|---|---|---|---|---|
| **Risk assessment** | X | X | X | X |
| **Risk treatment decisions** | | X | | X |
| **Security requirements definition** | X | X | X | X |
| **Control selection** | | | | X |
| **Control implementation** | | | | |

*TABLE 5.*The covered step of the ISSRM process by security languages

## IV. Discussion

Currently, various security modeling languages may be evaluated with the ISSRM domain model. The alignments mentioned in the article allow representing an IS using different constructs in order to ensure a better sustainability and interoperability. Still, the alignment does not refer to equivalence between the ISSRM model domain and the security modeling languages. It only describes the constructs that supports the ISSRM concepts. The mapping of the ISSRM domain model and the security modeling languages is not provided so it has been conducted subjectively.

SecureUML and Misuse Cases Diagrams cover the same steps of the ISSRM domain model (Assets identification, risk assessment and security objectives definition). Although, the distinction between the two is that SecureUML only describes information relevant to access control. Thus, it provides a system modeling from an administrator (protector) perspective. In contrast, Misuse Cases Diagrams provides a system modeling from the attacker point of view.

As for Mal-Activity Diagram, it enables like SecureUML and Misuse Cases Diagrams to cover assets identification, risk assessment and security objectives definition but also includes risk treatment decisions. Specifically, they detail a threat scenario, by describing the behaviors of the concerned actors.

Secure Tropos enables identification of critical assets and their relationships which is not the case with the other languages. Some Secure Tropos constructs only support partially the ISSRM concepts. Such as “Belief” which merely represents

“Vulnerability”. Secure Tropos deals with security risk management at a general level.

The alignment does not provide a complete secured model. None of these of alignments address security with a risk-driven approach. For some ISSRM concepts, alignment does not provide modeling constructs. Actually, no modeling construct is afforded for the concepts Risk and Risk treatment.

Finally, we identified that no inter-firm alignment like modeled in Figure 2 is elaborated. This would be a source of interesting findings in order to enrich the alignment concept.

Figure 3 reflects a diagram modeling the flow of communication between two organizations. For establishing the communication, a risk management unit is responsible for monitoring the communication. The risk management unit claim to each organization to authenticate and then specify the necessary parameters for the communication establishing. Not all communication requests can be accepted.

After establishing the communication, different threat scenarios can be triggered. For now, only two threats were modeled. The first threat concerns the failure of a critical asset of one of the organization. This failure will eventually trigger various other failures since each asset has its interdependencies. For that reason, the risk management unit plays a major role. It allows better determining the details of this failure and proposing the necessary countermeasures in order to address this failure as quickly as possible. The second threat “assetAdd” describes the request of adding a new asset required for the communication. Thus, adding a new element to the architecture of an organization also includes the risk of emergence of new vulnerabilities that can be exploited by threats. Also for this failure, risk management unit intervenes to manage the risks resulting.

Figure 4 shows the diagram outlined in Figure 3 but introduces the case where an organization (organization3) that didn’t join the communication already developed by the two first organization (organization1 and organization2) and a second case where an organization (organisation4) succeeded to join the communication. The access to the communication for organisation4 was firstly granted by the risk management unit and secondly by organization1 who first launched the communication. After the risk management unit analyzes the new risks that may influence the communication, it establishes the necessary treatments to alleviate their occurrences to the different participating entities.

In a perfect world, ERM would save organizations money, create stakeholder value, and facilitate growth through the exploitation of new opportunities. None of the mentioned security modeling languages "Mal-activity Diagrams, Misuse Case, Secure Tropos, SecureUML" is in fact suited to support the whole ISSRM process. They focuses generally on a limited steps of ISSRM and do not cover its full scope such as the

combine between business and IT. Another founded drawback is that these languages don't model the business and IS assets in a meaningful manner for ISSRM domain model. ERM approaches and related benefits are promising to fill these gaps.

## V. Conclusion and future work

Security issues related to IT services continue to be a big concern in today's society. Security risk management is not simply a technical problem any longer. The intention of this article was to compare security modeling languages with the ISSRM domain model and try combining the obtained results with the concept of ERM.

Given the central role of ISSRM alignment with security modeling languages, organizations need usage guidance. This semantic would help to extends information system security in order to fulfill secure business functions. This paper rewards the areas where efforts return most value.

The alignments discussed need improvement. Given that several ISSRM concepts are supported by the same security modeling languages concepts, a distinction should be proposed. It may also help the complete the coverage of the ISSRM concepts not supported.

No perfect support of the ISSRM concepts is provided. Each alignment incorporates limitations. To fully take advantage of these alignments, it is suitable to correct these limitations. Either by adding new constructs or by creating ontology that guides the constructs. It is also possible to conceive transforming rules that would lead from one alignment to another (like from SecureUML to Secure Tropos and vice versa). This will fully enhance interoperability between security modeling languages in the security risk management domain.

Another gap in the alignments discussed, we identified that most studies only investigate an alignment in a firm-internal context. No inter-firm alignment like modeled in Figure 2 is elaborated. This would be a source of interesting findings in order to enrich the alignment concept.

Organizations are subject to various risks and the ultimate goal of ERM is to model, measure, analyze, and respond to these risks in a holistic manner. A further research may be conducted in order to append ERM to ISSRM and adapt it to the telecom sector. Actually, when crutial business processes and strategic planning are aligned with proactive ISSRM process, a well-defined path and strategy to attain business value may be achieved.

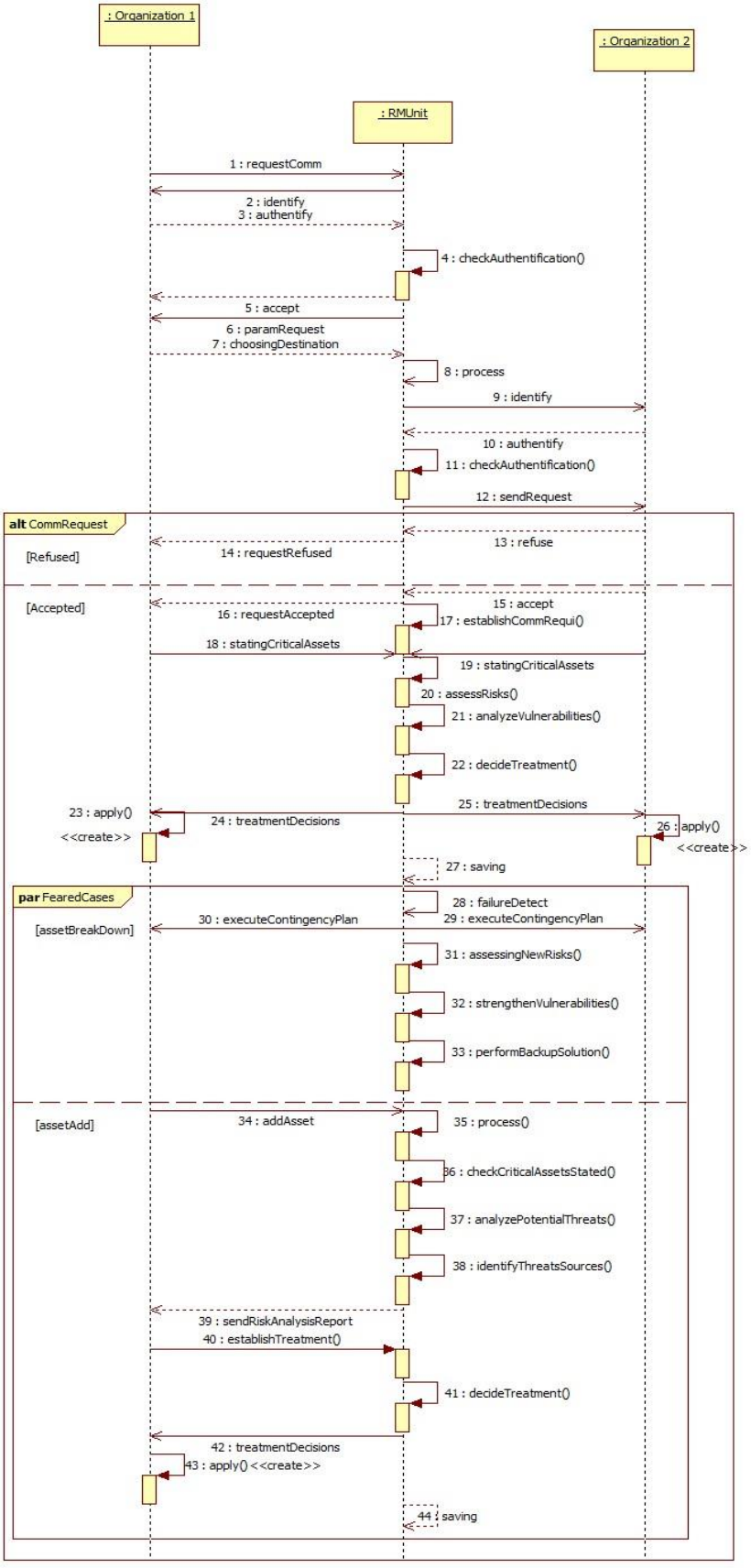


**Figure 3.** Inter-firm risk modeling

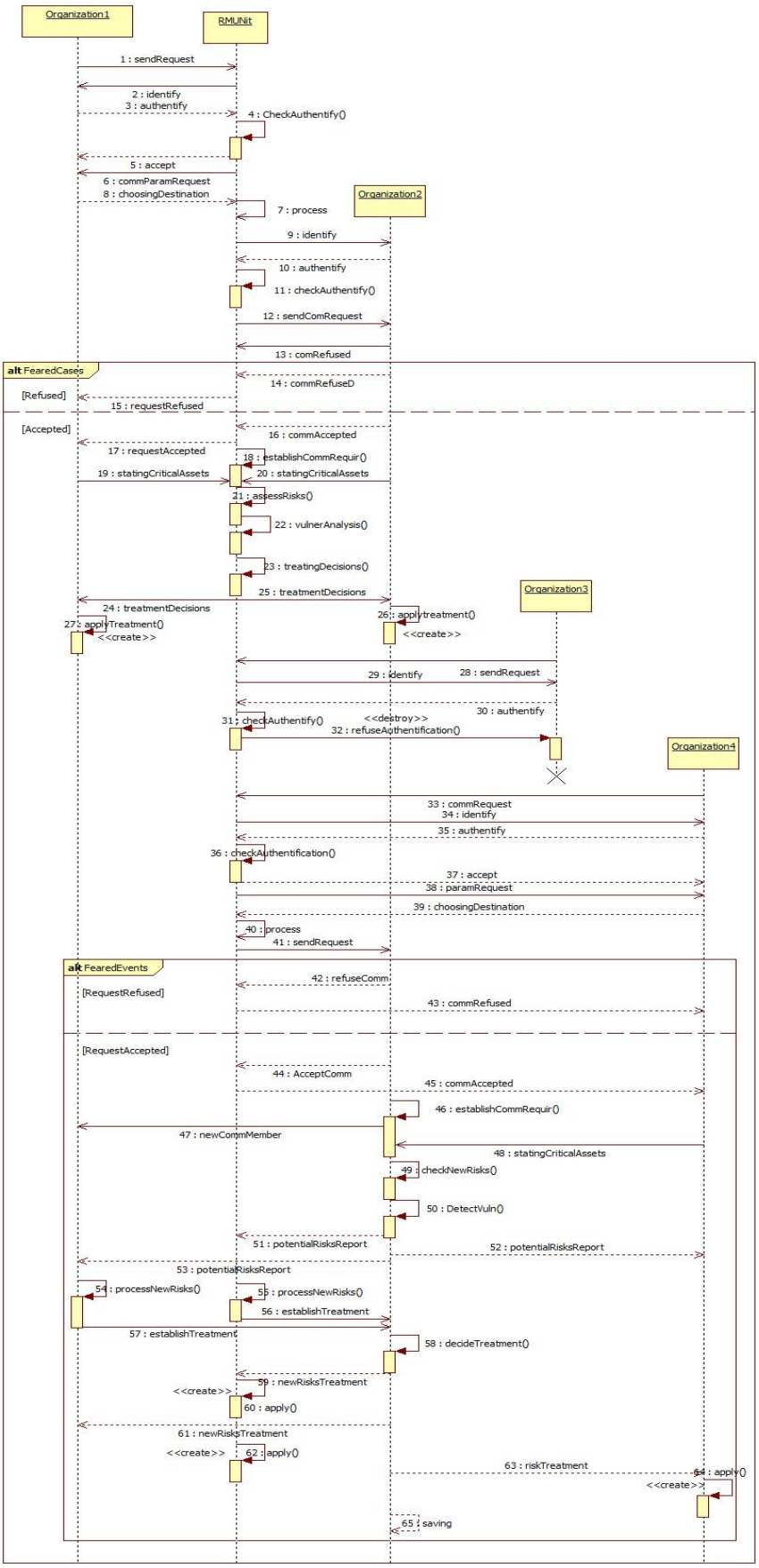


**Figure 4.** Inter-firm feared cases

## References


[1] J. M. Yusta, G. J. Correa, and R. Lacal-Ar ántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," Energy Policy, vol. 39, p. 6100–6119, Oct. 2011.

[2] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," Int. J. Crit. Infrastruct. Prot., vol. 8, p. 53–66, Jan. 2015.

[3] S. Alhawari, L. Karadsheh, A. Nehari Talet, and E. Mansour, "Knowledge-Based Risk Management framework for Information Technology project," Int. J. Inf. Manag., vol. 32, p. 50–65, Feb. 2012.

[4] H. Tohidi, "The role of risk management in IT systems of organizations," Procedia Comput. Sci., vol. 3, p. 881–887, 2011.

[5] V. L. Mihailescu, "Risk analysis and risk management using MEHARI," J. Appl. Bus. Inf. Syst., vol. 3, p. 143, 2012.

[6] H. HEMERY, W. AKMOUCHE, and F. TATOUT, "Utilisation de la methodologie EBIOS en securite globale," REE Rev. Lélectricité Lélectronique, p. 29–125, 2007.

[7] Z. Yazar, "A qualitative risk analysis and management tool-CRAMM," InfoSec Read. Room White Pap., 2002.

[8] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Pittsburgh PA Carnegie Mellon Univ., 2003.

[9] A. Goldstein and U. Frank, "Components of a multi-perspective modeling method for designing and managing IT security systems," Inf. Syst. E-Bus. Manag., vol. 14, p. 101–140, Feb. 2016.

[10] W. Abbass, A. Baina, M. Bellafkih, "Using EBIOS for risk management in critical information infrastructure", in 2015 5th World Congress on Information and Communication Technologies (WICT), Dec. 2015, Under publication.

[11] N. Mayer, A. Rifaut, E. Dubois, and others, "Towards a risk-based security requirements engineering framework," in Workshop on Requirements Engineering for Software Quality. In Proc. of REFSQ, 2005.

[12] É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management," in Intentional Perspectives on Information Systems Engineering, S. Nurcan, C. Salinesi, C. Souveyet, and J. Ralyté, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 289–306, 2010.

[13] N. Mayer, E. Dubois, R. Matulevicius, and P. Heymans, "Towards a measurement framework for security risk management," in Proceedings of modeling security workshop, 2008.

[14] T. Lodderstedt, D. Basin, and J. Doser, "SecureUML: A UML-based modeling language for model-driven security," in ≪ UML≫ 2002—The Unified Modeling Language, Springer, p. 426–441, 2002.

[15] M. J. M. Chowdhury, "Security risk modelling using SecureUML," p. 420–425, 2014.

[16] H. Mouratidis and P. Giorgini, "Secure tropos: a security-oriented extension of the tropos methodology," Int. J. Softw. Eng. Knowl. Eng., vol. 17, p. 285–309, 2007.

[17] D. Mellado, H. Mouratidis, and E. Fern ández-Medina, "Secure Tropos framework for software product lines requirements engineering," Comput. Stand. Interfaces, vol. 36, no. 4, pp. 711–722, Jun. 2014.

[18] J. Castro, M. Kolp, and J. Mylopoulos, "Towards requirements-driven information systems engineering: the Tropos project," Inf. Syst., vol. 27, p. 365–389, 2002.

[19] G. Sindre, "Mal-Activity Diagrams for Capturing Attacks on Business Processes," in Requirements Engineering: Foundation for Software Quality, vol. 4542, P. Sawyer, B. Paech, and P. Heymans, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 355–366, 2007.

[20] O. O. Mwambe, "Syntactic and Semantic Extensions of Malicious Activity Diagrams to Support ISSRM," Int. J. Comput. Appl., vol. 67, 2013.

[21] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," Requir. Eng., vol. 10, p. 34–44, Jan. 2005.

[22] F. Saleh and M. El-Attar, "A scientific evaluation of the misuse case diagrams visual syntax," Inf. Softw. Technol., vol. 66, p. 73–96, Oct. 2015.

[23] P. Bromiley, M. McShane, A. Nair, and E. Rustambekov, "Enterprise Risk Management: Review, Critique, and Research Directions," Long Range Plann., vol. 48, p. 265–276, Aug. 2015.

[24] W. Abbass, A. Baina, M. Bellafkih, "Survey on Information System Security Risk Management alignment ", in IEEE International conference on Information Technology for Organizations Development (IT4OD), Mar. 2016, Under publication.

[25] R. Matulevičius, N. Mayer, H. Mouratidis, E. Dubois, P. Heymans, and N. Genon, "Adapting secure tropos for security risk management in the early phases of information systems development," in Advanced Information Systems Engineering, p. 541–555, 2008.

[26] R. Matulevicius, H. Mouratidis, N. Mayer, E. Dubois, and P. Heymans, "Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management.," J UCS, vol. 18, p. 816–844, 2012.

[27] M. J. M. Chowdhury, R. Matulevičius, G. Sindre, and P. Karpati, "Aligning mal-activity diagrams and security risk management for security requirements definitions," in Requirements Engineering: Foundation for Software Quality, Springer, p. 132–139, 2012.

[28] I. Soomro and N. Ahmed, "Towards security risk-oriented misuse cases," in Business Process Management Workshops, p. 689–700, 2013.

[29] J. Viega and G. McGraw, Building secure software: how to avoid security problems the right way. Boston: Addison-Wesley, 2002.

[30] A. Bonnaccorsi. "On the Relationship between Firm Size and Export Intensity", Journal of International Business Studies, XXIII (4), p. 605-635, 1992.

[31] R. Caves. Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982.

[32] M. Clerc, M. "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm

Optimization". In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), p. 1951-1957, 1999.
[33] H.H. Crokell. "Specialization and International Competitiveness", in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986.
[34] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan. "A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II". KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000.